Извлекаем пароли из популярных программ

Денис Колисниченко , 25.04.2016 5 комментариев 140,693 Добавить в закладки



Содержание статьи

01. Браузеры
02. Почтовики
03. Не забываем о стариках
04. Как бороться

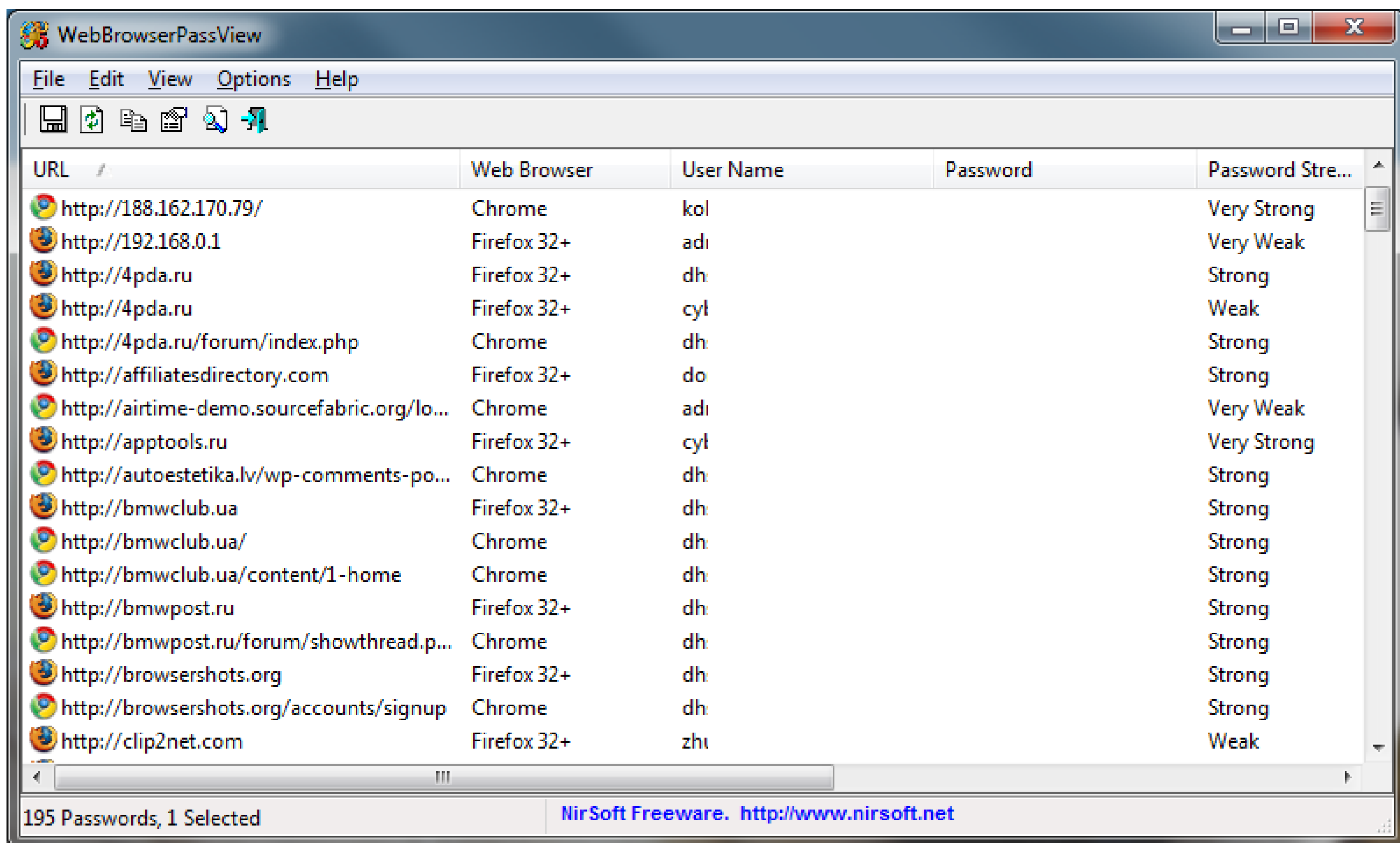
Браузеры, почтовые клиенты и другие программы часто предлагают сохранять пароли. Это очень удобно: сохранил и забыл, причем иногда в прямом смысле слова. Но что если тебе нужно сменить браузер, переустановить систему или просто зайти с другого компа? Оказывается, браузеры хранят пароли очень ненадежно. Программ для восстановления — масса, и конечно, на чужой машине они сработают ничуть не хуже, чем на твоей.

Браузеры

В браузере часто хранятся десятки, а то и сотни паролей. Понятное дело, если ты не используешь один пароль на все случаи жизни (а это не лучшая идея), запомнить пароли от всех сайтов и форумов бывает проблематично.

Если ты забыл важный пароль и не хочешь ломать себе голову, качай и ставь программу WebBrowserPassView. Ты будешь удивлен: она с легкостью извлечет пароли из Internet Explorer, Edge, Chrome, Opera, Safari, Firefox и Yandex Browser, причем поддерживаются самые новые версии. Лично я тестировал эту программу с IE, Firefox, Chrome и Opera — ни в одном случае не возникло осечек.

Перед запуском WebBrowserPassView желательно отключить антивирус, поскольку некоторые будут жаловаться, что это малварь. Результат восстановления показан на скриншоте. Не обессудь, но колонку Password и часть User Name я замазал.



Результат работы WebBrowserPassView

Выдели пароли, которые хочешь запомнить, выполни команду File — Save Selected Items. Выделенные пароли будут сохранены в обычный текстовый файл такого формата:

```
==================================================
URL                 : сайт
Web Browser         : Firefox 32+
User Name           : пользователь
Password            : пароль
Password Strength   : Very Strong
User Name Field     :
Password Field      :
Created Time        : 09.07.2015 21:15:16
Modified Time       : 09.07.2015 21:15:16
==================================================
```

И конечно, программа годится для извлечения паролей на чужой машине. Если у тебя есть локальный доступ или удаленный — через RDP или TeamViewer, то заполучить пароли будет несложно.

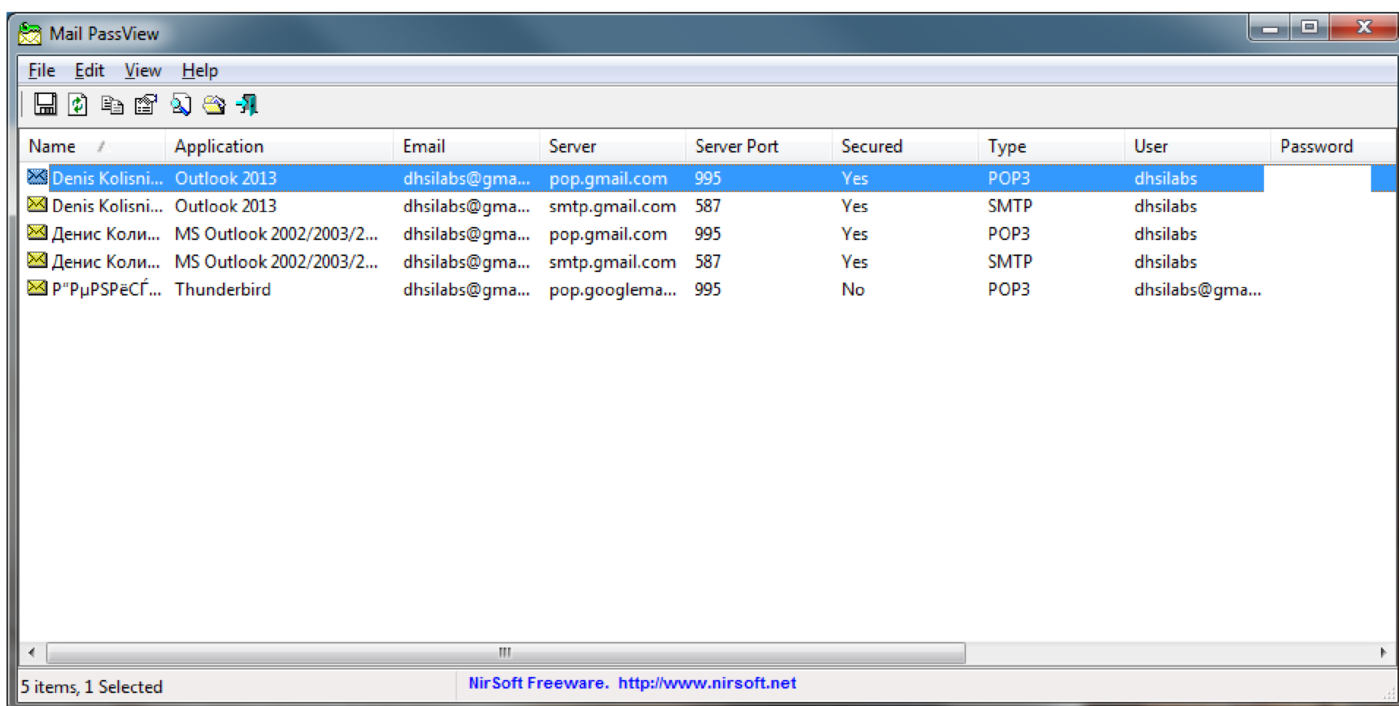
Почтовики

Аналогичные программы существуют и для восстановления паролей из почтовых клиентов. Одна из таких программ — Mail PassView. Она позволяет анализировать длинный список почтовиков:

- **Outlook Express;**
- **Microsoft Outlook 2000 (только учетные записи POP3 и SMTP);**
- **Microsoft Outlook 2002–2016 (учетные записи POP3, IMAP, HTTP и SMTP);**
- **Windows Mail;**
- **IncrediMail;**
- **Eudora;**
- **Netscape 6.x/7.x;**

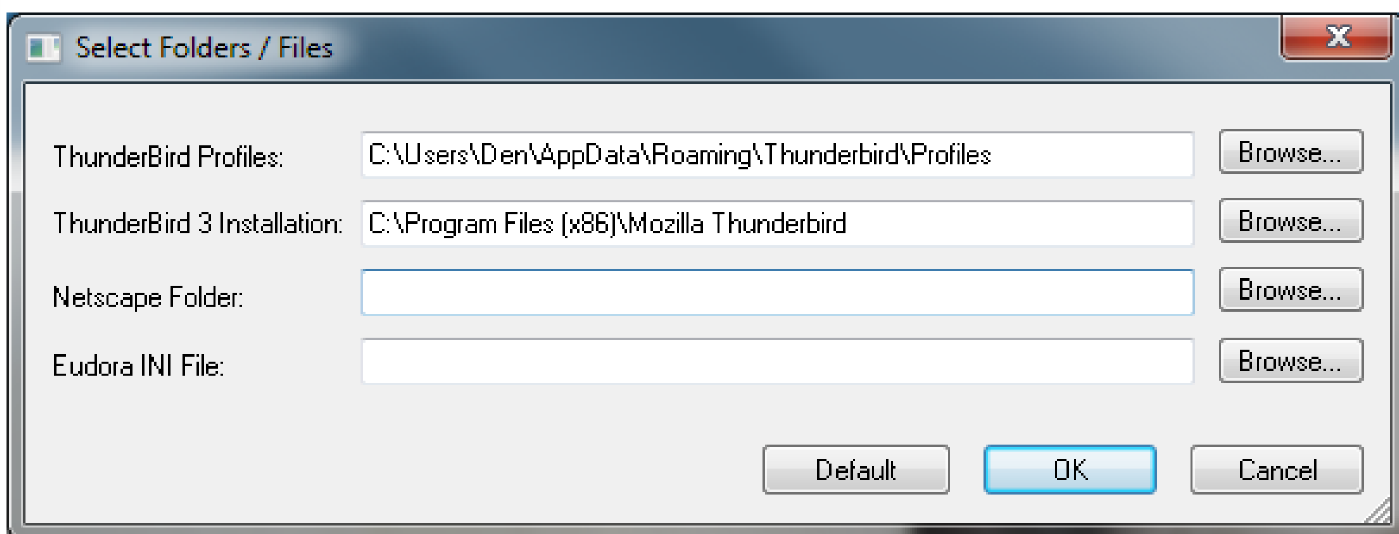
- Mozilla Thunderbird;
- Group Mail Free;
- Yahoo Mail — если пароль сохранен в приложении Yahoo Messenger;
- Hotmail/MSN mail — если пароль сохранен в приложении MSN Messenger;
- Gmail — если пароль сохранен в приложениях Gmail Notifier, Google Desktop или Google Talk.

Программа успешно восстановила мои пароли, сохраненные в Microsoft Outlook 2013 и Thunderbird.



Mail PassView

Если ты используешь portable-версии Thunderbird, Netscape и Eudora, то можно будет выбрать каталог с почтовиком.

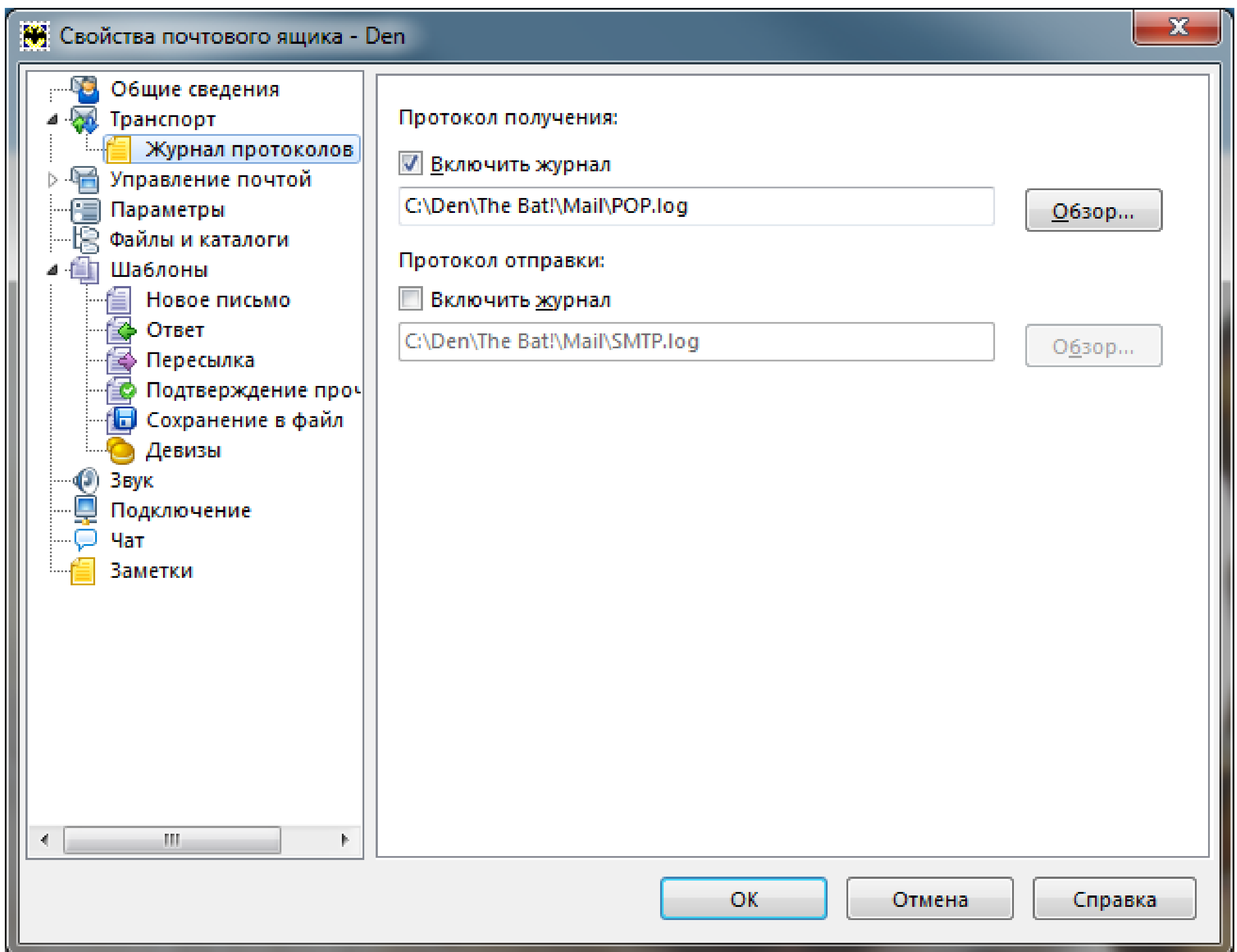


Выбор каталога для восстановления паролей из portable-версий почтовых клиентов

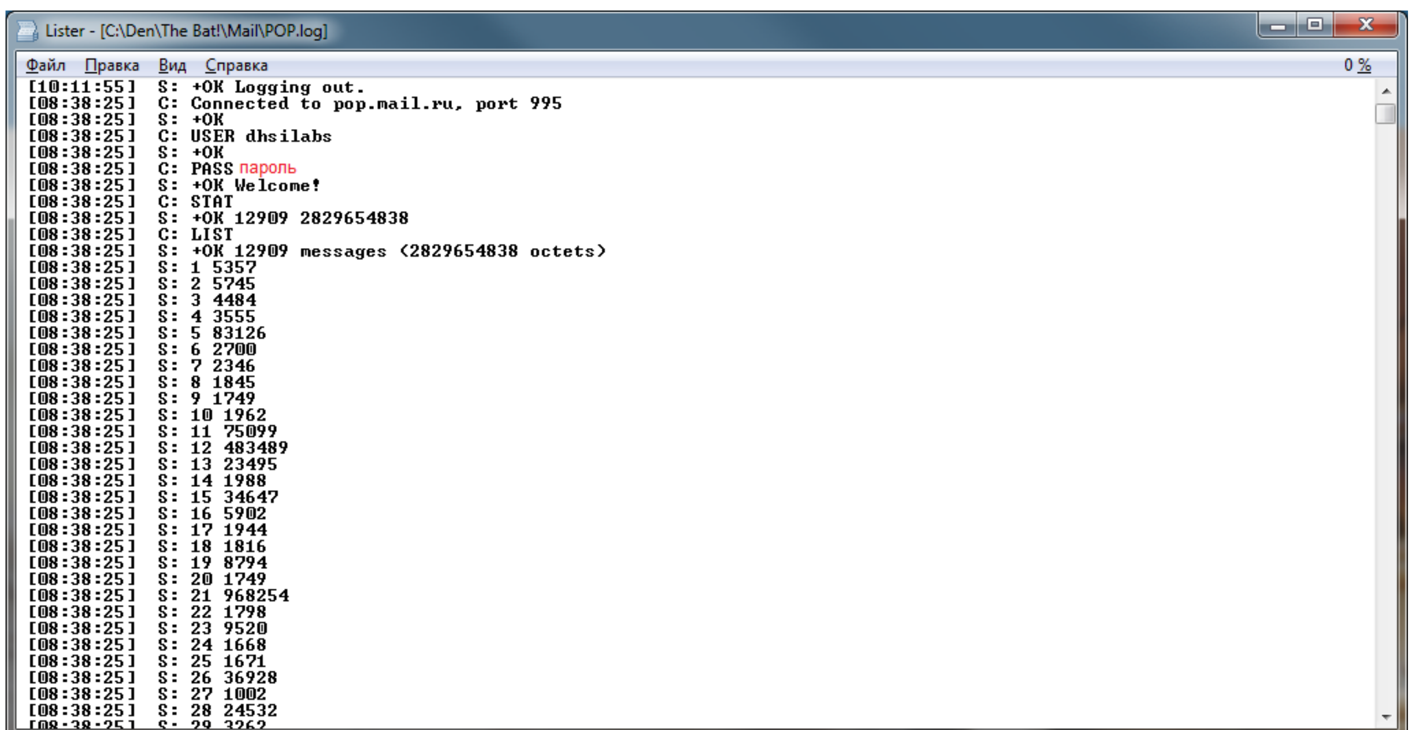
Не забываем о стариках

Mail PassView позволяет восстановить пароли из многих почтовых клиентов, но не из The Bat. Однако пользователям The Bat рано радоваться (или огорчаться — в зависимости от ситуации). Ведь этот почтовик сам может сообщить тебе сохраненный пароль!

Для этого нужно в настройках почтового ящика включить лог, а затем просмотреть файл `POP.log` после проверки почты (точнее — после подключения к POP-серверу). Как видишь, все предельно просто!



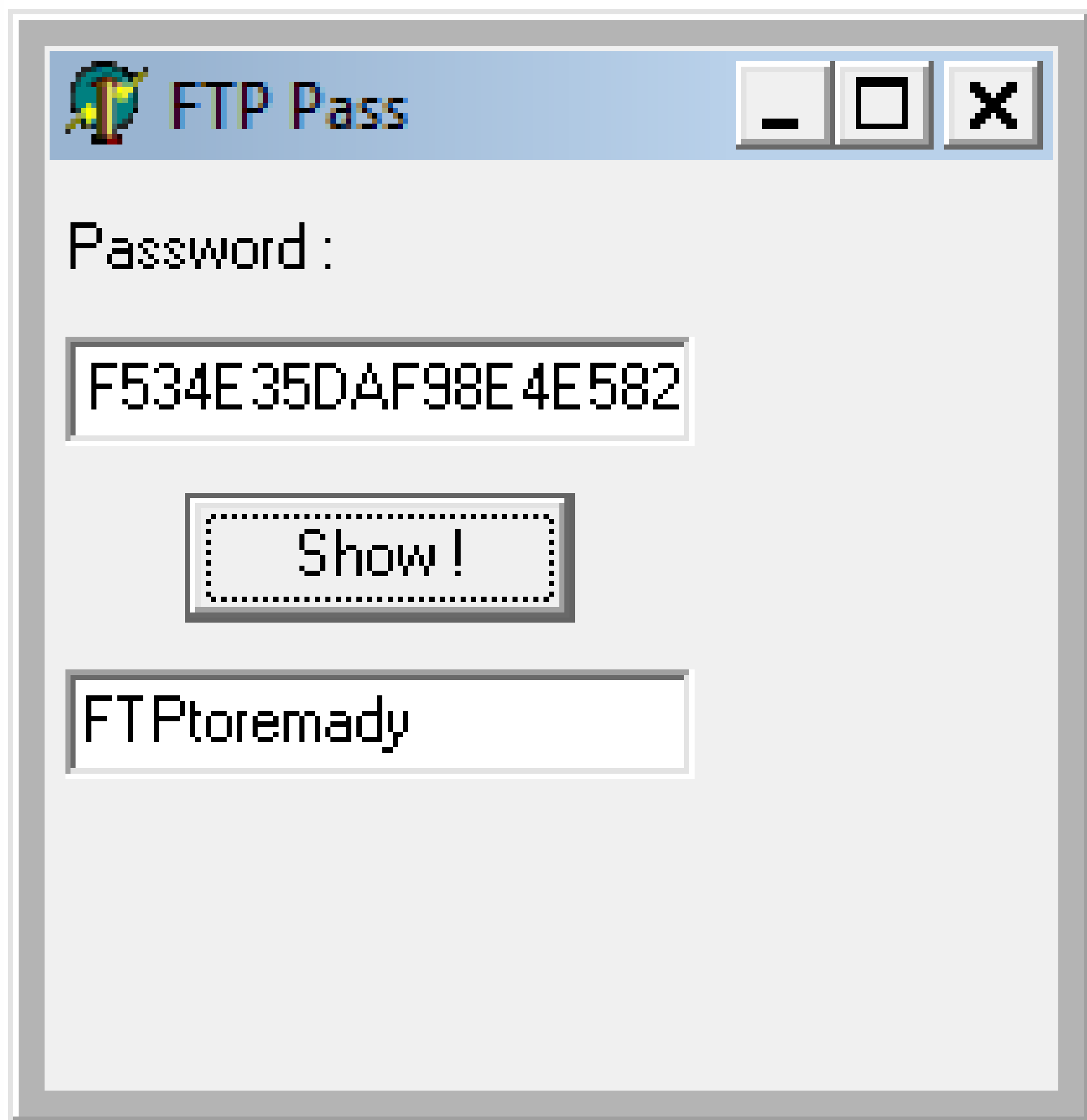
Включаем лог



Пароль передается в открытом виде командой PASS

Из другой популярной когда-то и встречающейся до сих пор программы — файлового менеджера Total Commander восстановить пароли чуть сложнее. Но если тебе вдруг надо выцарапать из него давно забытый пароль к FTP, то попробуй утилиту Windows Commander FTP crack.

Использовать эту утилиту нужно так. Ищешь `WCX_FTP.INI`, в нем хранятся зашифрованные пароли к FTP. Скопируй зашифрованный пароль в программу и нажми кнопку Show.



Утилита Windows Commander FTP crack

Кстати, из FileZilla тоже можно вытащить пароли — при помощи программы BulletsPassView.

Другие тулзы

Если рассмотренные программы по какой-то причине тебе не подойдут, то вот более полный список софта для восстановления паролей.

- **Outlook Password Decryptor — позволяет восстановить пароли из Outlook, в том числе последней версии — Outlook 2016 для 10.**
- **PstPassword — еще одна программа для восстановления паролей, сохраненных в Outlook.**
- **Dialupass — восстанавливает пароли от dial-up, RAS и VPN. Поддерживает Windows всех версий, начиная с 2000 и заканчивая десяткой.**

Кроме того, на сайте NirSoft ты найдешь много утилит для восстановления паролей. Подробно мы их все рассматривать не будем,

ограничимся выборочным списком.

- MessenPass — восстанавливает пароли из мессенджеров, таких как Miranda, Yahoo Messenger, ICQ Lite, Windows Messenger и другие. На данный момент все эти мессенджеры устарели, но вдруг тебе понадобится вытащить пароль от аськи со старого компа — MessenPass подойдет как нельзя лучше.
- IE PassView — старый просмотрщик паролей для IE, поддерживает версии до восьмой включительно, но лучше все же использовать WebBrowserPassView.
- BulletsPassView — позволяет восстановить пароли, сохраненные в различных приложениях для Windows, таких как CuteFTP, FileZilla, VNC.
- Network Password Recovery — восстанавливает пароли к расшаренным по сети папкам. Есть поддержка Windows 8 и Windows 10.
- PstPassword — позволяет восстановить пароль из файла PST. Работает с Outlook до версии 2007.
- PasswordFox, ChromePass, OperaPassView — восстанавливают пароли, сохраненные в Firefox, Chrome и Opera соответственно. Впрочем, WebBrowserPassView заменяет их все.
- WirelessKeyView — пригодится, если ты забыл сохраненный пароль к Wi-Fi. Хотя в этом, как правило, нет смысла, поскольку Windows этот пароль не охраняет, и ты в любой момент можешь просмотреть его, используя средства ОС.
- Remote Desktop PassView — достает пароли из файлов RDP.

Как бороться

Как видишь, многие программы предлагают сохранить пароли и почти никак их не защищают. Одни хранят их прямо в открытом виде, другие используют слишком слабое шифрование. Мне на моем компе удалось восстановить все пароли из всех браузеров и всех почтовых клиентов.

Что делать, если ты не хочешь, чтобы кто-то смог повторить это, добравшись до твоей машины? Есть разные способы решения этой проблемы. Самый лучший — никогда не сохранять пароли и не забывать пить таблетки для улучшения памяти. Специальные менеджеры паролей с гораздо более серьезной степенью защиты, чем у браузеров, — тоже неплохой выход. Ну а если все же хочешь сохранять пароли в браузере и почтовике, можешь скачать портативные версии и держать их на зашифрованном диске.

Оцени статью:





Денис Колисниченко

Постоянный автор журнала «Хакер»

Теги: FTP | Браузеры | Выбор редактора | Статьи | Утечки данных | Электронная почта